

(43)Date of publication of application : 25.01.2002

H04L 9/32  
G09C 1/00  
H04B 7/24  
H04Q 7/38  
H04L 12/28

(72)Inventor : NOGUCHI TETSUYA  
SHIMOTOONO SUSUMU

Figure 1 is a flowchart illustrating a secure communication system. It shows two parties, A and B, each with a public key and a private key. Party A sends a message to Party B, which is encrypted using A's public key. Party B then decrypts the message using A's private key. The diagram includes labels for '公開鍵' (Public Key), '秘密鍵' (Private Key), '送信' (Transmission), '受信' (Reception), '暗号化' (Encryption), and '復号化' (Decryption).

5/12/2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3552648

[Date of registration] 14.05.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP) (12) 特 許 公 報 (B2) (11) 特許番号

特許第3552648号

(73) 特許権者

(45) 発行日 平成16年8月11日(2004. 8. 11) (24) 登録日 平成16年5月14日(2004. 5. 14)

(51) Int. Cl.<sup>7</sup> H04L 9/00 F1 H04L 9/00 601C

請求項の 4 (全 16 頁)

(21) 出願番号 特願2000-184697 (P2000-184697) (73) 特許権者 390009531

(22) 出願日 平成12年6月20日(2000. 6. 20) インターナショナル・ビジネス・マシーン

(65) 公開番号 特願2002-26899 (P2002-26899A) ス・コーポレーション

(43) 公開日 平成14年1月25日(2002. 1. 25) INTERNATIONAL BUSIN

審査請求日 平成13年5月8日(2001. 5. 9) ESS MASCHINES CORPO

アメリカ合衆国10504 ニューヨーク

州 アーモンク ニュー オータワード

ロード

(70) 代理人 100085243

弁護士 坂口 博

(74) 代理人 100091568

弁護士 市位 嘉宏

最終頁に続く

(64) 【発明の名称】 アドホック無線通信用データ送受システム及びアドホック無線通信用データ送受方法

(57) 【特許請求の範囲】

【請求項 1】

各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存

在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキユアな

通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無

線通信機能付き携帯端末へ一方のユーザの公開鍵 K p が改ざんされることなく伝送された

ことが検証されると、公開鍵 K p は各ユーザにおいて無線通信機能付き携帯端末から無線

通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵

K p から共通鍵 K c を第 2 の生成アルゴリズムに基づいて生成し、一方のユーザの無線通

信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号

を用いて伝送されて来た情報を、前記公開鍵 K p に対応の秘密鍵を用いて復号し、この復

号後のデータに基づいて共通鍵 K c を第 2 の生成アルゴリズムから生成し、両無線通信機

能付きパソコンは、以降、共通鍵 K c に基づく暗号によりデータを送受することを特徴と

するアドホック無線通信用データ送受システム。

【請求項 2】

各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存

在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキユアな

通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無

線通信機能付き携帯端末へ一方のユーザの公開鍵 K p が改ざんされることなく伝送された

ことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵 K c を第 2 の

生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユー

ザの無線通信機能付き携帯端末から公開鍵 K p を用いて伝送されて来た情報を、前記公開

鍵 K p に対応の秘密鍵を用いて復号し、この復号後のデータに基づいて共通鍵 K c を第 2

の生成アルゴリズムから生成し、両無線通信機能付き携帯端末は、以降、共通鍵 K c に

基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受

システム。

【請求項 3】

各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存

在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキユアな

通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無

線通信機能付き携帯端末へ一方のユーザの公開鍵 K p が改ざんされることなく伝送された

ことが検証されると、公開鍵 K p は各ユーザにおいて無線通信機能付き携帯端末から無線

通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵

K p から共通鍵 K c を第 2 の生成アルゴリズムに基づいて生成し、一方のユーザの無線通

信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号

を用いて伝送されて来た情報を、前記公開鍵 K p に対応の秘密鍵を用いて復号し、この復

号後のデータに基づいて共通鍵 K c を第 2 の生成アルゴリズムから生成し、両無線通信機

能付きパソコンは、以降、共通鍵 K c に基づく暗号によりデータを送受することを特徴と

するアドホック無線通信用データ送受方法。

【請求項 4】

各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存

在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキユアな

通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無

線通信機能付き携帯端末へ一方のユーザの公開鍵 K p が改ざんされることなく伝送された

ことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵 K c を第 2 の

生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユー

ザの無線通信機能付き携帯端末から公開鍵 K p を用いて伝送されて来た情報を、前記公

開鍵 K p に対応の秘密鍵を用いて復号し、この復号後のデータに基づいて共通鍵 K c

を第 2 の生成アルゴリズムから生成し、両無線通信機能付き携帯端末は、以降、共通鍵 K c

に基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受

方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、伝送データの改ざんに対処するアドホック無線通信用データ送受システム及び

アドホック無線通信用データ送受方法に関するものである。

【0002】

【従来の技術】

アドホック無線通信のような特定のインフラを利用しないその場限りの近距離無線通信に

おいて不特定の二者が、データを意図の第三者により改ざんされることなく、伝送する場

合には、意図の第三者に知られることのない暗号鍵を共有する必要がある。しかしながら

、通信時に暗号鍵の値を固定する方法は煩雑であり、特に通信相手が初

顔合わせ等の状況下では、通信相手同士が口頭やメモ等により暗号鍵を共有することはほ

んど実用性がない。自動的に暗号鍵を共有する方法として、まず公開鍵を共有して、暗号

鍵をその公開鍵で暗号化した共有する方法がある。しかし、マン・イン・ザ・ミドル・ア

タック (Man-in-the-middle attack: マン・イン・ザ・ミドル・アタック) の詳細については、ジョン・ウィリアム・アンド・サンズ会社 (John Wi

ley & Sons, Inc) 出版の著書ブルース・シュナイアー (BRUCE S

C

10

HNEIER)の題名:応用暗号学(APPLIED CRYPTOGRAPHY)のp. 48~p. 50を参照されたい。)のリスクがある。

[0003]

マン・イン・ザ・ミドル・アタックにおけるデータ改ざんのリスクを軽減する。図1はアドホック無線通信システム10において送信元Aと送信先Bとが気が付かないまままで両者の間に悪意の第三者Cが介在する余地を示している。AとBとは、(a)のように、両者間に直接、通信路が開通されていると、思っている。Man-in-the-Middle Attack"がどのような場合に発生しているのか、具体的に例を挙げて説明する。

[0004]

無線暗号通信路開設の一般的な手順は以下になる。

手順1:送信元は不特定多数の相手に向かって、通信したい送信先のIDで呼びかける。  
手順2:送信先が無線接続可能な範囲に居れば、その呼びかけられたID(つまり自分のID)を受信する。

手順3:送信先は、自己の動作条件等を送信元に伝える。

手順4:通信路開設のために必要な動作パラメータ(利用する通信路の選択と設定、暗号鍵の交換等)を両者で決定する。

手順5:通信路開設し、相互通信が開始される。

[0005]

悪意の第三者が図1のCの位置に最も入り込み易いのは、盗聴の対象となる二者が対面で無線通信を開始するタイミングである。つまり、上記の列挙された手順1~3に介入する。図2及び図3は悪意の第三者が図1のCの位置に入り込む手口の一例を示す。電波の性格上、送信元Aは周囲のすべての送信先候補に特定IDで呼びかけざるを得ない(手順1)。

送信先Bは、自分のIDでの呼びかけが聞こえるので(手順2)、送信元Aに応答する(手順3)。ここで、悪意の第三者は自分以外のIDへの呼びかけに反応したり、自分以外のIDで呼びかけを行ったりして、下記のような成りすましを図ろうとする。まず、

悪意の第三者Cは送信先Bの応答に同一周波数帯のノイズをぶつけて送信元Aがその応答を聞き取れないようにする。この時点で、送信先Bはそのノイズの事実を知らないで、上記手順4に遷移して送信元Aからの手順4におけるセッショを開始している。送信元Aは手順4には居ないが、送信先Bはタイムアウト後に再度、自分のIDの呼びかけを聞く状態に戻る。一方、送信元Aは送信先Bからの応答が得られないので、タイムアウト後に再度同じIDで呼びかける(手順1)のが普通である。つまり、送信元Aと送信先Bは互いの手順の同期を取り始めようとして、それぞれのタイムアウトでその失敗に気が

つき、元の状態に戻るようになる。

[0006]

悪意の第三者Cは、送信元Aが再度同じIDで呼びかけるタイミングに合わせて待機し、さらに送信先Bが再度自分のIDの呼びかけを聞き始めるタイミングにも合わせて待機する。以後、悪意の第三者Cは送信元Aの呼びかけに送信先Bに成りすまして応答し、反対に自分のIDの呼びかけを聞き始めた送信先Bに送信元Aに成りすまして呼びかけを行う。勿論、悪意の第三者CはどのようなIDにも自分のIDを変化させる能力を有している。

上記で送信元Aと送信先Bが互いの手順の同期はすれから元の状態に戻るのとは同一時刻ではないので、このような二つの成りすまし行為を悪意の第三者Cは実行可能である。なぜなら、送信元Aと送信先Bがそれぞれ次のイベントで待機し始める時刻がそもそも異なるし、タイムアウトの対象となるイベントも異なるのでタイムアウト期間自身も異なるからである。

[0007]

この成りすまし工作によって、送信元Aは、正規の送信先Bから正常な応答があったと思っ

て、通信路開設手順、つまり手順4より悪意の第三者Cと一緒に通信路開設手順に同じく第三者Cと一緒に、正規の送信元Aからの呼びかけだと思っ

て、通信路開設手順に同じく第三者Cと一緒に

に遷移する。上記手順5まで進むと、二者のみで通信路を確保したと思っている両者A、

50

Bの機器の保有者に知られることなく悪意の第三者Cが互いの間で通信データを中継する形で盗聴することが可能になる。この成りすまし(中継)を利用すれば、例えばAがBに送るはずの公開鍵をCが改ざんして、Cが予め用意した秘密鍵に対応した公開鍵Aとすり替えることができる。これによって、本来AとBの間に構築された暗号通信路はAとCの間でのみ有効になり、CとBの間はCが別に設定した暗号通信路となる。つまり、Aから送られた暗号化データはCで復号化され、再度CとBの間の暗号化通信路用に別の暗号化通信路を通じて伝送される。その逆の伝送も同様である。AとBは共に通常手順で暗号化通信路を確立しているが、途中で公開鍵をすり替えられ、そのすり替えに気がつかないことで、盗聴される結果となる。このような攻撃(成りすましによる盗聴)をMan-in-the-middle attackと呼ぶ。暗号化通信路自身は安全であるから、このような攻撃への対処として、通信する両者で本間に同一の公開鍵を共有しているか否かを確保にすることが所要となる。

[0008]

【発明が解決しようとする課題】

Man-in-the-middle attackの対処法としては、認証機関の発行する証明書を利用して、証明書内に記載された個人ID(通常相手の名前等)を送元、伝送先で表示し視視比較することも考えられる。しかし、これには、証明書の発行にコストがかかる。また、認証機関を利用する場合、身元を登録して認証を行うため、通信相手に自分の身元を公開することになり、匿名性を保つことができないという問題も存在する。さらに、イエローページ(Yellow Page)のように公開鍵から利用者を特定するサービスを用いる場合は、電話回線等によるセキュアなネットワーク接続が必要であり、トランザクションコストがかかる。

[0009]

本発明の目的は、アドホック無線接続により相互に接続されるデータ送受装置間でデータを送受する場合において、通信相手へのなりすましによるデータの改ざんを有効に防止できるアドホック無線通信用データ送受システム及びアドホック無線通信用データ送受方法を提供することである。

本発明の他の目的は、口頭やメモ書きによるパスワードの取り交わしを省略でき、身元公開してしまふ認証機関を利用せず、能率的に、円滑に、かつ正確に通信相手を検証することのできるアドホック無線通信用データ送受システム及びアドホック無線通信用データ送受方法を提供することである。

[0010]

【課題を解決するための手段】

本発明のアドホック無線通信用検証システム及び方法によれば、アドホック無線接続により相互に接続される2個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになって

いる。

[0011]

両データ送受装置の距離は、両データ送受装置の検証データ出力部における検証データを相互に対比する必要があるもので、典型的には、両データ送受装置間をユーザ(利用者)が数秒で行き来できる10m以内等であり、好ましくは数mである。検証データ生成用データに基づいて生成した検証データには検証データ生成用データそのものであってもよいとする。検証データは、両データ送受装置の検出データ出力部における検証データが相互に一致しているか否かの判定が行い易いものに設定される。一般には、両データ送受装置において起動されている検証用ソフトが同一であれば、検証データ生成用データから検証データの生成のために同一の生成アルゴリズムが使用される。しかし、複数値の生成アルゴ

リズムの内の1個を、両データ送受装置のユーザがその場において適宜、取り決めたりするようになるっていいよ。

【0012】一方のデータ送受装置は、送信した検証データより第1の生成アルゴリズムに基づいて検証データを生成する。他方のデータ送受装置は、受信した検証データより第1の生成アルゴリズムに基づいて検証データを生成する。そして、両データ送受装置の抽出データと出力部から出力される検証データが一致するか否かの判定を行い、一致していれば、検証データと生成用データが、途中において改ざんされることなく、一方のデータ送受装置から他方のデータ送受装置へ正しく伝送されていること、すなわちデータの完全性が検証されたことになる。このように、データの完全性を能率的に実施でき

【0013】  
本発明のアドホック無線通信用検証システム及び方法によれば、検証データは、視覚的又は聴覚的な検証データである。

【0014】  
視覚的な検証データには、画像、数値、文字、又はそれらの組み合わせがある。検証データの視覚表示の例としては、検証データが例えば計数ビットのビットデータである場合には、 $x$ 、 $y$ 、 $z$  ビットを、連続する等ビットずつで区分し、 $x$  軸方向へ区分、 $y$  軸方向へ各区分ごとに数値とするヒストグラムがある。検証データの聴覚表示の例としては、前述のヒストグラムの各区分の数量に対応する高さの音を、低位の区分から順番に出力するものである。検証データは、両データ送受装置における検証データの一致及び不一致が円滑かつ正確に判定し易いものが選択されるのが好ましい。

【0015】  
本発明のアドホック無線通信用検証システム及び方法によれば、検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになってい

線形座標系での出力形態では、面データ受送装置におけるもの同士が類似していても、検座標系での出力形態では相違が明確であり、あるいはその逆の場合がある。線形座標系での出力形態及び面データの出力形態の両方が対比されることにより、一致及び不一致の判定の正確性が高まる。

【0017】  
本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子  
が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一  
又は異なる一方向性関数に係る演算子を1個以上、直列に並べた直列演算子列を除け、該  
直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応  
値が検証データとされる。

【0018】一方方向性関数には、例えばハッシュ関数 (Hash Function) がある。上記定義した演算子列には、演算子が1個しかないものも含んでいる。検証データ生成用データから検証データへの検証データ生成に一方方向性関数を関与させることにより、検証データから検証データ生成用データを見つけ出す困難性が増大し、悪意の第三者が真の検証データ生成用データに類似の偽の検証データ生成用データを使って、データ改ざんをする可能性が低下する。なお、検証データの偽の検証データ生成用データを見つけて出すことは、直列演算子列の長さが増えればなる程、計算量的に不可能となる。

**【0019】**

本発明のアドホック無線通信用検証システム及び方法によれば、第1の生成アルゴリズムで検証データを送受信する際に、各検証データについて、両データ送受信装置は、検証データを複製し、生成するものであり、各検証データについて、両データ送受信装置は、検証データを出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。この検証データを用いて、送信側と受信側の両方で検証が行われる。

50

複数個の検証データ全部が類似している可能性は極めて低い。検証データを複数個、生成し、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一対一一致するか否かを判定されることにより、検証の正確性が向上する。

【00021】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、膨張算子及び作用する数値を膨張算子の入力、膨張算子の演算結果を膨張算子の出力と定義し、同一又は異なる一方向性関数に依る演算子を2個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された2個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、前データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【0.0.2.2】本発明のアドホック無線通信用検証システム及び方法によれば、閾値を演算子、膨演算子及び作用する数値を膨演算子の入力、膨演算子の演算結果を膨演算子の出力と定義し、相互に異なる一方向性閾値に係る演算子を複数、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力を又それぞれ検証データとし、各検証データの出力と、演算子データ送受装置の検証データ出力値とを相互に一致させるか否かを判定されるようになっている。

【0023】  
本発明のアドホック無線通信用検証システム及び方法によれば、検証データ生成用データは一方のデータ送受装置の公開鍵である。

【0024】  
検証データ生成用データが一方のデータ送受装置の公開鍵であれば、検証データの検証に  
よって、他方のデータ送受装置が受信した公開鍵が一方のデータ送受装置の公開鍵であるこ  
とを検証することができる。したがって、他方のデータ送受装置から一方のデータ送受装  
置へ一方のデータ送受装置の公開鍵を用いた暗号通信により例えば井田鍵等を送る等して  
面データ送受装置間の井田鍵による暗号通信の開設を完全に実現できる。

【0025】  
前述のアドホック無線通信回路システムを利用する本発明のアドホック無線通信回路システムは、各ユーザにより所有する無線通信機に付し携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機に付し携帯端末と無線通信機能付きパソコンとはセキヤ通信路で結ばれており、アドホック無線通信システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ伝送されたことが検知される。公開鍵 K p は各ユーザにおいて無線通信機能付きパソコンは、共通鍵 K c を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵に由来する暗号を用いて伝送されて来た情報に基づいて、共通鍵 K c に基づく暗号によりデータを送受する。

[illegible]

50

cを第2の生成アルゴリズムから生成し、次に、共通鍵Kcは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づき暗号によりデータを送受する。

【0027】

本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Kpが改ざんされることなく伝送されたことが検証されること、公開鍵Kpは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Kpから共通鍵Kcを第2の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Kcを第2の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づき暗号によりデータを送受する。

【0028】

本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Kpが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Kcを第2の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Kcを第2の生成アルゴリズムから生成し、次に、共通鍵Kcは各ユーザにおいて無線通信機能付きパソコンから無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づき暗号によりデータを送受する。

【0029】

各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとのセキュアな通信路とは、例えば、各ユーザの秘密鍵による相互通信により確立される。無線通信機能付き携帯端末はPDA(Personal Digital Assistant)と呼ばれるものを含む。ビジネスマンの仕事のスタイルの一例としての隠しコンピュテーティング(Hidden Computing)：発明の実施の形態において詳述)が考えられている。隠しコンピュテーティングでは、例えばノートPC等の無線通信機能付きパソコン同士で、改ざんなくデータの送受が行われることが望まれる。このようなケースにおいて、ユーザは無線通信機能付き携帯端末の検証データ出力部における検証データの対比から一方の無線通信機能付き携帯端末の公開鍵Kpが途中で改ざんされることなく他方の無線通信機能付き携帯端末へ伝送されたことが検証され、その検証を両ユーザの無線通信機能付きパソコンへ引き継がせ、両無線通信機能付きパソコンの間で共通鍵Kcにより暗号通信を円滑に実施できる。

【0030】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものである。

：アドホック無線接続により相互に接続される2個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【0031】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものでさらに付加される。

：記録媒体。

：検証データは、視覚的又は聴覚的な検証データである。

【0032】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものでさらに付加される。

：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。

【0033】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものでさらに付加される。

：関数を演算し、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を1倍以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【0034】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものでさらに付加される。

：第1の生成アルゴリズムは、検証データを複数値、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【0035】

【発明の実施の形態】

以下、発明の実施の形態について図面を参照して説明する。

図4はデータ完全性の検証及びそれに続く暗号データ伝送の全体のプロローチャートである。暗号通信開設要求側及び被要求側をそれぞれ伝送元及び伝送先と定義し、図4では、伝送元データ送受装置をA、伝送先データ送受装置をBとしている。データ完全性検証のための公開鍵の伝送元及び伝送先と、データ完全性検証後の本伝送(ほんでんそう)：共通鍵を使った暗号伝送)の伝送元及び伝送先とは、一致している必要はなく、逆であってもよいし、また、データ完全性検証後の本伝送では、伝送元及び伝送先は適宜、入れ替わってもよい。

【0036】

図4の処理を順番に説明する。

(a) Aは、Bに暗号通信開設要求と共に自分の公開鍵Kp、及び検証データ生成アルゴリズムを指定するID(以下、このIDを「ID1」と言う。)を送信する。Aは、同時に、自分の公開鍵Kpを元に検証データXpを生成する。

(b) BがAからAの公開鍵Kpとして受信したデータをKxとする。もし、AからBへの無線伝送路においてデータの改ざんがなければ、 $Kx = Kp$ となり、改ざんがあれば、 $Kx \neq Kp$ とは別ものとなる。BはAから受け取ったKxを元に、Aより指定のあったID1の検証データ生成アルゴリズムで検証データXxを生成する。検証データの例は、後述の図5において詳述する。

(c) A、Bのユーザは、A及びBの表示部にそれぞれ出力表示された検証データXp、Xxが同一であるか否かを検証する。もし、 $Xp = Xx$ であれば、 $Kx = Kp$ を意味し、A-Bの通信路にはデータ完全性があるとの判断を下す。

(d) BはAから受信した公開鍵Kpを使って、共通鍵生成のための乱数値Rと共通鍵生成アルゴリズムを指定するID(以下、このIDを「ID2」と言う。)とを暗号化して、Aへ送信する。ID2については、A、Bが同一の通信ソフトを使用する等、ID2が固定されているならば、ID1と同様に、A-B間の伝送は省略できる。Bは、同時に乱



数値Rから共通鍵生成アルゴリズムを用いて共通鍵Kcを生成する。

(e) A は B から受信した暗号化された乱数値 R を、公開鍵 K<sub>p</sub> に対応する秘密鍵 K<sub>s</sub> を使って復号し、乱数値 R と ID2 とを得、乱数値 R から ID2 の共通鍵生成アルゴリズムを用いて共通鍵 K<sub>c</sub> を生成する。

(f) 以降、 $A-B$ は、共通鍵 $K_c$ に基づく暗号化通信によりデータを送受する。

【0037】

例、A、Bの検証データ出力部に表示する検証データは検証データ生成用データそのもの、例えばAの公開鍵そのものであってもよい。すなわち、A、Bの検証データ生成用データに、Aの公開鍵がビット表示される。しかし、教値は、暗み取り難いので、公開鍵の教値生成用データは、公開鍵を画像表示して変換してもよい。図5は検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す。検証データ生成用データがAの公開鍵であるとして、図画像表示部27に報費表示される。検証データ生成用データがAの公開鍵であるとして、公開鍵をLSBからMSBまでを等しいビット数の区域に順番に区切り、検証を区域、鍵域を各区域の教値とするヒストグラムで、検証データが表されている。もし、Aの公開鍵Kがp倍、伝送路の途中で悪意の第三者により成りすまして行われているならば、BがAより受信した検証データ生成用データKxは、検証データ生成用データKpに等しいので、 $Xx = Xp$ となる。したがって、A及び/又はBのユーザ、又は信頼できる他の検証者は、A、Bの表示部を直接、見て、A、Bの表示部に表示されているXp及びXxを対比（比較）し、両者が一致していれば、AからBへAの公開鍵がそのまま伝送されて来たたと判断し、すなわち完全性があると判断し、両者が不一致であれば、AからBへの伝送中にデータ改ざんがあったと判断する。

100381

しかし、人間の認識能力の精度は必ずしも高くなく、図5のようなヒストグラムと比較画像を単純に生成しただけではハミングディスタンスの小さい類似公開鍵との違いを検出してきかない場合がある。そこで、公開鍵に対してハッシュ関数等の一方方向性関数を適用して所定のデータまで変換し、それをヒストグラム等の検証画像の表示を行ってもよい。この場合、成りすまして行おうとする第三者が類似するデータを出力できない。ただし、作成する検証画像の情報量が公開鍵のビットサイズに比べて極めて小さい場合、全数探索によって破られる可能性はある。そのような条件下では、すでに一方方向性関数を適用したデータに対してさらに一方方向性関数を適用して新たなデータを算出したり、別の一方方向性関数を公開鍵に適用して、新たなデータを算出したりして、別の検証画像を生成する。この操作を繰り返すことで、複数の検証画像を生成することであり、これを用いることで成りすましてはならない。この検証画像を生成することによって、公開鍵の強度をあげることができ、これを検証画像の強度とすることができる。

100391

検証データは、ヒストグラムのような画像に限定されず、文字データの表示や音階の強化などをめざし、それらの複数のデータを組み合わせて提示して、ユーザに対して提示したりしてもよい。概念的な検証データとしては、図5のヒストグラムの縦軸方向の値を音の高低又は音色に対応させ、図6の横軸方向の左の区域から順番に所定時間ごとに各区域の値に対応する音を出力する。また、検証データを視覚表示器と放音手段としてのスピーカとの両方から出力させるようにしてもよい。

00401

図6～図8は一方方向性関数を使用して検証データ生成用データから検証データを生成する方式をそれぞれ示している。データD1は検証データ生成用データを意味し、データD2、D3、D4、...は検証データを意味する。また、各一方方向性関数は、演算子として機能し、入力に作用して、演算結果を出力する。一方方向性関数は例えばハッシュ関数(Hash Function)である。

0041]

図6では、1回目は検証データとしてデータD1に一方方向性関数Fを作用させ、データD2を得る。2回目は、データD2に同一の一方方向性関数Fを作用させ、データD3を得る。

なわち、一方性関数Fを含むループを形成し、データD3を得る。以降、ループ処理を繰り返し、D4、D5、...を得る。所定回数のループを繰り返した後、最終的な演算結果をDnとし、このDnを検証データとして、最終的な演算結果Dnのみにデータ送受装置20（図10）の検証画像表示部27に視覚表示する。最終的な演算結果Dnのみデータ送受装置20の検証画像表示部27に視覚表示するだけでなく、D2、D3、D4、...の特定の幾つ又は全部をデータ送受装置20の検証画像表示部27に画面分割又は時分割で視覚表示させることにし、表示されたそれぞれについて対比してもよい。複数の検証データを対比することにより、たとえばそれらの1個の検証データについて一致、不一致の判定ができるが紛らわしくても、対比される複数の検証データのすべてについて一致、不一致の判定を向上でき、紛らわしくなる可能性は極めて小さく、データ改ざんについての検証の正確性を向上できる。

00421

なお、D2, D3, D4, . . . の全部でなく、特定の幾つかのみを対比する場合に、その幾つかについての組み合わせ (Subset) を適宜、変更するようにしておくことにより、照像の第三者の攻撃に対する防衛強度は高くなる。

【0043】

図7では、相互に異なる複数個の方向性関数  $F, G, H, \dots$  を用ゐし、共通のデータ D1 に各一方向性関数  $F, G, H, \dots$  を作用させ、各演算結果 D2, D3, D4,  $\dots$  を得る。D2, D3, D4,  $\dots$  の特定の幾つか又は全部を検証データとして、データ送受装置 20 の検証画像表示部 27 に画面分割又は時分割で複重表示させ、表示されたそれらについて列示。

【0044】

図8では、相互に異なる複数個の一方方向性関数 $F, G, H, \dots$ を用数する。1回目には、検証データ生成用データとしてのデータD1に一方方向性関数 $F$ を作用させ、データD2を得る。2回目は、データD2に一方方向性関数 $G$ を作用させ、データD3を得る。こうして、次に前段の演算結果に次段の一方方向性関数を作用させ、複数個のD2, D3, D4,  $\dots$ を得る。D2, D3, D4,  $\dots$ の特定の幾つか又は全部を検証データとして、図8の方式にデータ送受装置20の検証面像表示部27に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。なお、図6における複数個対比の方式は、図8の方式において、相互に異なる一方方向性関数を使用する代わりに同一の一方方向性関数を使用した特殊の例と考えることができる。

【0045】

図9は図6～図8の処理を組み合わせて検証データを示すブロック図である。図6～図9の検証データ演算方式をそれぞれタイプ(Type)1, 2, 3と定義している。図8の左端の検証データ生成用データが入力され、図8の右端に検証データが出力される。図8の左端の例列はタイプ1, 2, 3から2個以上のタイプを選択し、それらを任意の順に並べて検証データ生成用データを得ることができ、図9の例列は一例である。

[0046]

図10はデータ送受装置20のブロック図である。データ送受装置20は、場合により伝送元Aになったり、伝送先Bになつたので、伝送元としての構成と伝送先としての構成を兼備している。データ送受装置20がAである場合には、伝送検証部24は、自分の公開鍵を検証画像生成部26へ出力し、また、データ送受装置20がBである場合には、通信部25において検証画像生成部26へ受信したAからの送信データ31として受信したデータの公明鍵を検証部27に送り、検証画像生成部26へ送られる。検証画像生成部26は伝送検証部24から受け取った検証データを生成し、生成された検証データは検証画像表示部27に提示される。A、Bの所有者等のユーザは、アドホック無線接続されている2個のデータ送受装置20の検証画像表示部27における検証データと対比し、一致及び不一致を確認する。その結果を検証結果入力部28に入力する。ユーザからの検証結果入力部28への入力結果は伝送検証部24へ通知され、伝送検証部24は、両検証データが相互に一致しているかどうかを検査する場合には、AからBへアドホック無線接続の際の伝送路を介して伝送したものと通知を受ける。

数値 R から共通鍵生成アルゴリズムを用いて共通鍵 K c を生成する。

(e) A は B から受信した暗号化された乱数値 R を、公開鍵 K<sub>p</sub> に対応する秘密鍵 K<sub>s</sub> を使って復号し、乱数値 R と ID2 とを得、乱数値 R から ID2 の共通鍵生成アルゴリズムを用いて共通鍵 K<sub>c</sub> を生成する。

(f) 以降、 $A-B$ は、共通鍵 $K_c$ に基づく暗号化通信によりデータを送受する。

【0037】

例、A、Bの検証データ出力部に表示する検証データは検証データ生成用データそのもの、例えばAの公開鍵そのものであってもよい。すなわち、A、Bの検証データ生成用データに、Aの公開鍵がビット表示される。しかし、教値は、暗み取り難いので、公開鍵の教値生成用データは、公開鍵を画像表示して変換してもよい。図5は検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す。検証データ生成用データがAの公開鍵であるとして、図画像表示部27に報費表示される。検証データ生成用データがAの公開鍵であるとして、公開鍵をLSBからMSBまでを等しいビット数の区域に順番に区切り、検証を区域、鍵域を各区域の教値とするヒストグラムで、検証データが表されている。もし、Aの公開鍵Kがp倍、伝送路の途中で悪意の第三者により成りすまして行われているならば、BがAより受信した検証データ生成用データKxは、検証データ生成用データKpに等しいので、 $Xx = Xp$ となる。したがって、A及び/又はBのユーザ、又は信頼できる他の検証者は、A、Bの表示部を直接、見て、A、Bの表示部に表示されているXp及びXxを対比（比較）し、両者が一致していれば、AからBへAの公開鍵がそのまま伝送されて来たたと判断し、すなわち完全性があると判断し、両者が不一致であれば、AからBへの伝送中にデータ改ざんがあったと判断する。

100381

しかし、人間の認識能力の精度は必ずしも高くなく、図5のようなヒストグラムと比較画像を単純に生成しただけではハミングディスタンスの小さい類似公開鍵との違いを検出してきかない場合がある。そこで、公開鍵に対してハッシュ関数等の一方方向性関数を適用して所定のデータまで変換し、それをヒストグラム等の検証画像の表示を行ってもよい。この場合、成りすまして行おうとする第三者が類似するデータを出力できない。ただし、作成する検証画像の情報量が公開鍵のビットサイズに比べて極めて小さい場合、全数探索によって破られる可能性はある。そのような条件下では、すでに一方方向性関数を適用したデータに対してさらに一方方向性関数を適用して新たなデータを算出したり、別の一方方向性関数を公開鍵に適用して、新たなデータを算出したりして、別の検証画像を生成する。この操作を繰り返すことで、複数の検証画像を生成することであり、これを用いることで成りすましてはならない。この検証画像を生成することによって、公開鍵の強度をあげることができ、これを検証画像の強度とすることができる。

100391

検証データは、ヒストグラムのような画像に限定されず、文字データの表示や音階の強化などをめざし、それらの複数のデータを組み合わせて提示し、ユーザに対して提示したりしてもよい。概念的な検証データとしては、図5のヒストグラムの縦軸方向の値を音の高低又は音色に対応させ、図6の横軸方向の左の区域から順番に所定時間ごとに各区域の値に対応する音を出力する。また、検証データを視覚表示器と放音手段としてのスピーカとの両方から出力させるようにしてもよい。

00401

図6～図8は一方方向性関数を使用して検証データ生成用データから検証データを生成する方式をそれぞれ示している。データD1は検証データ生成用データを意味し、データD2、D3、D4、...は検証データを意味する。また、各一方方向性関数は、演算子として機能し、入力に作用して、演算結果を出力する。一方方向性関数は例えばハッシュ関数(Hash Function)である。

0041]

図6では、1回目は検証データとしてデータD1に一方方向性関数Fを作用させ、データD2を得る。2回目は、データD2に同一の一方方向性関数Fを作用させ、データD3を得る。

開鍵についてデータ完全性があると判断する。次に、データ送受装置20がBである場合には、乱数生成部34において乱数値が生成され、共通鍵生成部33では、乱数生成部34において生成された乱数値からID2の共通鍵生成アルゴリズムにより共通鍵を生成する。一方、乱数生成部34が生成した乱数値及びID2が復号化・暗号化実装部32においてAの公開鍵に基づいて暗号化され、その暗号データDcが送受信部31を介してAへ送られる。また、乱数値RからID2の生成アルゴリズムに基づいて共通鍵を生成し、それを鍵保存部35に保存する。データ送受装置20がAである場合には、Bから伝送されて来た暗号データDcの送受信部31を復号化・暗号化実装部32において自分の秘密鍵により復号し、乱数値R及びID2を得、乱数値RからID2の共通鍵生成アルゴリズムに基づいて共通鍵を生成し、該共通鍵を鍵保存部35に保存する。以降は、データを送信する場合は、鍵保存部35から共通鍵を引き出して、該共通鍵に基づいて送信データを暗号化・暗号化実装部32において暗号化し、送受信部31として相手方へ送信する。データを受信する場合は、受信した暗号化された送受信部31を復号化・暗号化実装部32において復号し、平データをハードディスク（図示せず）等に保存したり、所定の処理を行ったりする。

#### 【0047】

図11は伝送元A側の通信処理のフローチャートである。公開鍵Kpを送信（S40）、該公開鍵KpからID1の検証データ生成アルゴリズムにより検証データXpを生成し（S42）、検証データXpを検証画像表示部27に出力する（S44）。S46では、自分の検証データXpと伝送先Bの検証データXxとを対比して、同一と判断されれば、S48へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、伝送先Bからの乱数値Rの受信を待ち（S48）、S50において、乱数値Rを受信したと判断すると、S52へ進み、乱数値受信待ち時間が所定時間経過したにもかかわらず、乱数値Rの受信のないときは、エラーとして該プログラムを終了する。S52では、伝送先Bからの乱数値Rの暗号データを前記公開鍵Kpに対応の自分の秘密鍵で復号して、乱数値Rを得る。A、Bのデータ送受装置間では検証データの共通鍵生成アルゴリズムについてそれぞれIDが予め取り決められており、送信先Bにおいて今回の共通鍵生成アルゴリズムとして採用されたID（例では、ID2）が乱数値Rと一緒に伝送先Bから伝送元Aへ送信されて来ている。こうして、S56では、乱数値RからID2の共通鍵生成アルゴリズムに基づいて送信先Bとの通信用の共通鍵を生成し、以降、該共通鍵を用いてBと暗号化通信を開始する（S58）。

#### 【0048】

図12は伝送先B側の通信処理のフローチャートである。伝送元Aから公開鍵Kxを受信する（S60）。この受信した公開鍵は、A、B間の伝送路に悪意の第三者が介在していると考えられている可能性があるかもしれないので、Kxではなく、Kxと表現することにする。次に、送信元Aから公開鍵Kpと一緒に送られて来たID1で指定された検証データ生成アルゴリズムによりKxから検証データXxを生成し（S62）、検証データXxを検証画像表示部27に出力する（S64）。S66では、自分の検証データXxと伝送元Aの検証データXpとを対比して、同一と判断されれば、S68へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、乱数値Rを生成し（S68）、乱数値Rと、乱数値の共通鍵生成アルゴリズムの中から、今回、選択した共通鍵生成アルゴリズムのIDとしてのID2とを送信元Aの公開鍵により暗号化したデータを送信元Aへ送信し（S70）、ID2の共通鍵生成アルゴリズムに従って共通鍵Kcを生成し（S72）、以降、該共通鍵を用いてAと暗号化通信を開始する（S74）。

#### 【0049】

図13は隠れコンピュータ・ディタリングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。隠れコンピュータ・ディタリング（Hidden Computing）とは、ユーザは、コンピュータを隠等に納め、手元のPDA（携帯情報端末：Personal Digital Assistant）等の携帯機器から無線

50

通信等を利用して該コンピュータを遠隔操作する利用形態を意味する。PDA80a等に装備されている82は通信デバイスである。上記に述べたような公開鍵のデータの完全性を確認できるシステムを装備していない機器（＝図86a、86bの中のノートパソコン88a、88b）間でアドホック無線通信を行う場合において、これらノートパソコン88a、88bと事前にセキュアな通信路90a、90bを確保している暗号通信路開設プロトコルを実装したPDA80a、80bを用いて、間接的に暗号通信路を開設する。なお、PDAとノートパソコンとの間のセキュアな通信路は、例えば両者間で事前に取り決められている共通鍵による暗号通信により達成される。図13においてまず手前（a）で通信路84をPDA80a、80b間で開設して、一方のPDAの公開鍵を他方のPDAへ伝送して、該公開鍵のデータ完全性を検証する。次に、手前（b）においてPDA80a、80b間のデータ完全性を検証を、それぞれのPDA80a、80bとセキュアな通信路90a、90bにより接続されているノートパソコン88a、88bへ継承する。この継承は、具体的に、PDA80a、80b間でデータ完全性を検証された公開鍵をセキュアな通信路90a、90bを介してノートパソコン88a、88bを伝送することにより達成される。以降、ノートパソコン88a、88bは、両者間の通信路92を介して共通鍵を共有した後、該共通鍵による暗号でデータを送受する。

#### 【図面の簡単な説明】

【図1】送信元Aと送信先Bとが気が付かないまま両者の間に悪意の第三者Cが介在する余地を示す図である。

【図2】悪意の第三者が図1のCの位置に入り込む手口の一例の第1の部分を示す図である。

【図3】悪意の第三者が図1のCの位置に入り込む手口の一例の第2の部分を示す図である。

【図4】データ完全性の検証及びそれに続く暗号データ伝送の全体のフローチャートである。

【図5】検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す図である。

【図6】一方向性関数を使用して検証データ生成用データから検証データを生成する第1の方式を示す図である。

【図7】一方向性関数を使用して検証データ生成用データから検証データを生成する第2の方式を示す図である。

【図8】一方向性関数を使用して検証データ生成用データから検証データを生成する第3の方式を示す図である。

【図9】図6～図8の処理を組み合わせて検証データを求める方式を示すブロック図である。

【図10】データ送受装置のブロック図である。

【図11】伝送元A側の通信処理のフローチャートである。

【図12】伝送先B側の通信処理のフローチャートである。

【図13】隠れコンピュータ・ディタリングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。

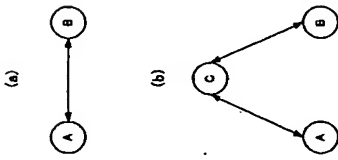
#### 【符号の説明】

10 アドホック無線通信システム  
80a、80b PDA（無線通信機能付き携帯情報端末）  
88a、88b ノートパソコン（無線通信機能付きパソコン）

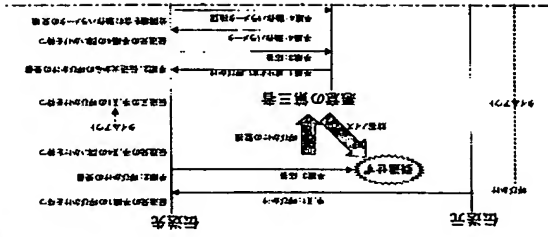
40



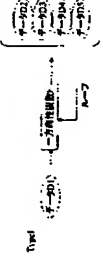
【図 1】



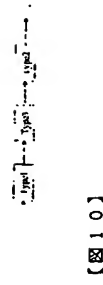
【図 2】



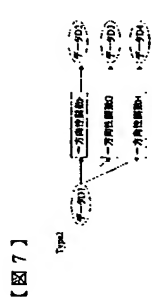
【図 6】



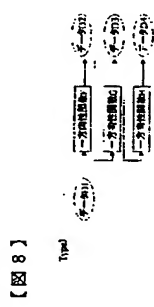
【図 9】



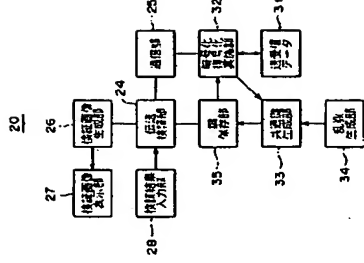
【図 10】



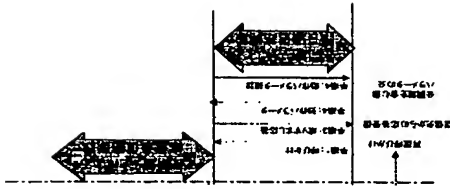
【図 7】



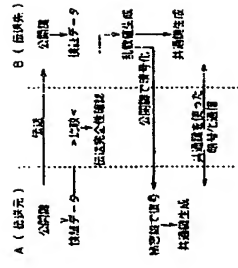
【図 8】



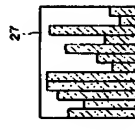
【図 3】



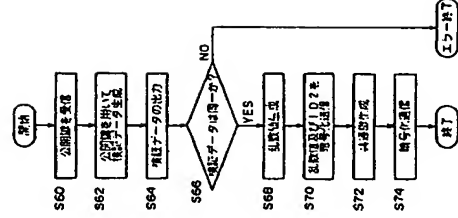
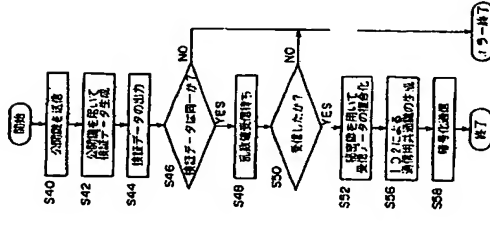
【図 4】



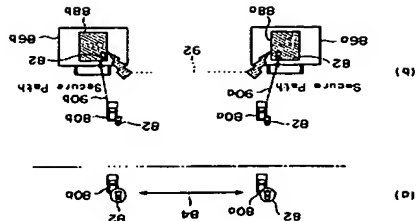
【図 5】



【図 12】



【図13】



フロントページの続き

(72)発明者 野口 哲也  
神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内  
(72)発明者 下越野 享  
神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内

審査官 中里 裕正

(56)参考文献 特開平06-244832 (JP, A)  
特開2000-10927 (JP, A)

(58)調査した分野(Int.Cl.<sup>7</sup>, DB名)  
H04L 9/08